IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

TITLE:

METHOD FOR INCORPORATING FACIAL RECOGNITION TECHNOLOGY IN A MULTIMEDIA SURVEILLANCE SYSTEM

INVENTOR:

DAVID A. MONROE

CROSS REFERENCE TO RELATED APPLICATION

[00] This application claims the priority of U.S. Provisional Application Serial No. 60/428,096, filed on November 21, 2002.

BACKGROUND OF THE INVENTION

Field of the Invention.

[01] The invention generally relates to use of facial recognition technology as used in surveillance and access systems and is specifically directed to incorporation of such technology in an IP compatible, networked, comprehensive multimedia surveillance system.

Discussion of the Prior Art.

[02] My earlier patents and applications have covered various aspects of the networked multimedia surveillance system in detail. My following earlier patents and pending applications are incorporated herein by reference:

Serial # 10/192,870 Filing Date: 07/10/2002
Title: Comprehensive Multi-Media Surveillance and Response System for Aircraft, Operations Centers, Airports and Other Commercial Transports, Centers and Terminals

Serial # 08/738,487 Filing Date: 10/28/1996
Patent # 5,798,458 Issue Date: 08/25/1998
Title: Acoustic Catastrophic Event Detection and Data Capture and Retrieval System for Aircraft

Serial # 08/745,536 Filing Date: 11/12/1996
Patent # 6,009,356 Issue Date: 12/28/1999
Title: Wireless Transducer Data Capture and Retrieval System for Aircraft

Serial # 08/815,026 Filing Date: 03/14/1997
Patent # 5,943,140 Issue Date: 08/24/1999
Title: Method and Apparatus for Sending and Receiving Facsimile Transmissions Over a Non-Telephonic Transmission System

Serial # 09/143,232 Filing Date: 08/28/1998
Title: Multifunctional Remote Control System for Audio Recording, Capture, Transmission and Playback of Full Motion and Still Images

Serial # 09/257,448 Filing Date: 02/25/1999
Title: Multi-Casting Communication Protocols for Simultaneous Transmission to Multiple Stations

Serial # 09/257,720 Filing Date: 02/25/1999
Patent # 6,392,692 Issue Date: 05/21/2002
Title: Network Communication Techniques for Security Surveillance and Safety System

Serial # 09/257,765 Filing Date: 02/25/1999
Patent # 6,366,311 Issue Date: 04/02/2002
Title: Record and Playback System for Aircraft

Serial # 09/257,767 Filing Date: 02/25/1999
Patent # 6,246,320 Issue Date: 06/12/2001
Title: Ground Link With On-Board Security Surveillance System for Aircraft and Other Commercial Vehicles

Serial # 09/257/769 Filing Date: 02/25/1999
Title: Ground Based Security Surveillance System for Aircraft and Other Commercial Vehicles

Serial # 09/257,802 Filing Date: 02/25/1999
Patent # 6,253,064 Issue Date: 06/26/2001
Title: Terminal Based Traffic Management and Security Surveillance System for Aircraft and Other Commercial Vehicles

Serial # 09/593,901 Filing Date: 06/14/2000
Title: Dual Mode Camera

Serial # 09/594,041 Filing Date: 06/14/2000
Title: Multimedia Surveillance and Monitoring System Including Network Configuration

Serial # 09/687,713 Filing Date: 10/13/2000
Title: Apparatus and Method of Collecting and Distributing Event Data to Strategic Security Personnel and Response Vehicles

Serial # 09/966,130 Filing Date: 09/21/2001
Title: Multimedia Network Appliances for Security and Surveillance Applications

Serial # 09/974,337 Filing Date: 10/10/2001
Title: Networked Personal Security System

Serial # 09/715,783 Filing Date: 11/17/2000
Title: Multiple Video Display Configurations and Bandwidth Conservation Scheme for Transmitting Video Over a Network

Serial # 09/716,141 Filing Date: 11/17/2000
Title: Method and Apparatus for Distributing Digitized Streaming Video Over a Network

Serial # 09/725,368 Filing Date: 11/29/2000
Title: Multiple Video Display Configurations and Remote Control of Multiple Video Signals Transmitted to a Monitoring Station Over a Network

Serial # 09/853,274 Filing Date: 05/11/2001
Title: Method and Apparatus for Collecting, Sending, Archiving and Retrieving Motion Video and Still Images and Notification of Detected Events

Serial # 09/854,033 Filing Date: 05/11/2001
Title: Portable, Wireless Monitoring and Control Station for Use in Connection With a Multi-Media Surveillance System Having Enhanced Notification Functions

Serial # 09/866,984 Filing Date: 05/29/2001
Title: Modular Sensor Array

Serial # 09/960,126 Filing Date: 09/21/2001
Title: Method and Apparatus for Interconnectivity Between Legacy Security Systems and Networked Multimedia Security Surveillance System

Serial # 10/134,413 Filing Date: 04/29/2002
Title: Method for Accessing and Controlling a Remote Camera in a Networked System With Multiple User Support Capability and Integration to Other Sensor Systems

[03] Several companies have developed computer algorithms that are capable of producing a "digital signature" from video images of people's faces. These signatures are much like a fingerprint: they are unique to individuals; they are relatively small so they are efficient; and, they may be used in databases to look up the identity and other data about the person.

[04] While other types of biometrics, such as iris scanning, are at best or even more accurate than facial recognition (which has a relatively low error rate; just under 1 percent), facial recognition will probably be accepted more widely because it is not intrusive. Further, it does not require that the user push, insert or click on anything. Companies often do not need to install anything beyond the new software because most already have cameras in place and pictures of employees on file -- making it less expensive than iris reading setups. In addition, the relatively small size of the database for a facial profile makes it an attractive technology.

[05] One example of a currently available facial recognition software is the Visionics' FaceIt system. The FaceIt software measures a face according to its peaks and valleys -- such as the tip of the nose, the depth of the eye sockets -- which are known as nodal points. A typical human face has 80 nodal points and precise recognition can be achieved with as few as 14 to 22 utilizing the FaceIt system. Specifically, the FaceIt system concentrates on the inner region of the face, which runs from temple to temple and just over the lip, called the 'golden triangle.' This is the most stable because even if facial hair such as a beard is altered, or if the subject changes or adds glasses, changes in weight or ages substantially the 'golden triangle' region tends to not be affected, while places such

as under chin would be substantially altered. FaceIt plots the relative positions of these points and comes up with a long string of numbers, called a faceprint.

[06] Visage Technology of Littleton, Massachusetts, has a slightly different model. Its software compares faces to 128 archetypes it has on record. Faces are then assigned numbers according to how they are similar or different from these models. The Visage Technology has been utilized to date in the identification of criminals, for access control, for transaction security and for identity fraud prevention.

[07] Most recently, government and aviation officials are poised to begin using facial recognition systems to scan airport terminals for suspected terrorists. Recently, Visionics has teamed up with a domestic airline to demonstrate a conceptual boarding system that will use FaceIt to facilitate the rapid boarding of the airline's frequent flyers.

[08] In the past, law enforcement officials often have no more than a facial image to link a suspect to a particular crime or previous event. Up to now, database searches were limited to textual entries (i.e., name, social security number, birth date, etc.), leaving room for error and oversight. By conducting searches against facial images, the facial recognition technology permits rapid review of information and quickly generated results, with the ability to check literally millions of records for possible matches, and then automatically and reliably verifying the identity of a suspect.

[09] The facial recognition technology has several advantages over other biometric systems. For example, with facial recognition technology a person can be identified at a distance or in a crowd. The technology has the capability of capturing a face in the field of view, extract the face from the background data and compare it against a database.

[10] The system permits the creation of watch lists or the like. This could include, for example, known shoplifters, terrorists or criminals, as well as frequent customers, VIP's, expected visitors or individuals generally classified as friends or foes. The system can be used at airports, casinos, public buildings, schools, subways, colleges, factories, business facilities, housing complexes, residences and the like.

[11] The system also is useful in transaction modes. Customers are used to being verified or being recognized by their face at retail locations by providing merchants with a driver's license or other form of photo ID. In sharp contrast to today's widely used signature verification process, which is highly unreliable and cannot be accurately determined by unskilled and untrained clerks, face recognition makes verification reliable, automatic and fast. In banking, facial recognition technology can adapt to already installed ATM cameras for recognizing and verifying customer identities so the financial transaction can be quickly and effortlessly conducted. Such technology can replace reliance on alphanumeric PINs to identify and authenticate a user.

[12] Face recognition is the only biometric that can be used in two modalities - logon and continuous monitoring. An example of logon modality is use as a perimeter defense mechanism, where an authorized individual gains entry to a network or session after a one-time logon process. This is the typical mode for all biometric systems. In addition, face recognition supports a continuous monitoring mode where persons are continuously authenticated for ensuring that at all times the individual in front of the computer or handheld device continues to be the same authorized person who logged in.

[13] Currently available technology focuses on the following aspects of facial recognition:

Detection - When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. A multi-scale algorithm is used to search for faces in low resolution. The system switches to a high-resolution search only after a head-like shape is detected.

Alignment - Once a face is detected, the system determines the head's position, size and pose to assure that the face is appropriately turned toward the camera for the system to register it.

Normalization - The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose. Normalization is performed regardless of the head's location and distance from the camera.

Representation - The system translates the facial data into a unique code. This coding process allows for easier comparison of the newly acquired facial data to stored facial data.

Matching - The newly acquired facial data is compared to the stored data and linked to at least one stored facial representation.

[14] The heart of current facial recognition systems is the algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a faceprint, a unique numerical code for that face. Once the system has stored a faceprint, it can compare it to the thousands or millions of faceprints stored in a database. In the FaceIt system, each faceprint requires an 84-byte file. The FaceIt system can match multiple faceprints at a rate of up to 60 million per minute. As comparisons are made, the system assigns a value to the comparison using a scale of 1 to 10. If a score is

above a predetermined threshold, a match is declared. The operator then views the two photos that have been declared a match to be certain that the computer is accurate.

[15] As the facial recognition technology develops, expanding uses are desirable. A comprehensive, system approach incorporating this technology with other legacy, digital and IP system architectures is needed. A comprehensive, coordinated approach utilizing this technology with known surveillance techniques and with system collection, distribution and management techniques will be required to maximize the value of this and other biometric recognition technologies.

SUMMARY OF THE INVENTION

[16] The subject invention is directed to the integration of facial recognition capability into a multimedia security system with IP compatibility for enhancing the collection, distribution and management of recognition data by utilizing the system's cameras, databases, monitor stations, and notification systems.

[17] In its simplest configuration, a camera views a scene of interest, and a processor analyzes the video signals produced by the camera. The processor performs the steps of:

- Facial Separation, e.g., locating human faces within the viewed scene,
- Facial Signature generation, e.g., deriving a unique identifying descriptor for the detected faces,
- Database Creation, adding said descriptors and separated facial image to a comparison database,
- Database Lookup, matching the captured descriptors with previously-captured faces or images containing faces or other relevant data, and
- Generating alarms as appropriate.

[18] The basic function of the system can be enhanced by dividing the processing function processors. One or more processors perform the computationally intensive tasks of Facial Separation and Facial Signature generation, while yet another processor performs the less demanding task of database pattern matching. This yields improved system economies and flexibility. Cameras and Facial Processors may be added incrementally to the system as needed, and as is unnecessary for each Facial Processor to contain or to access the entire 'reference' database.

[19] In the subject invention, the basic facial recognition technology is incorporated into a networked surveillance system. In the preferred embodiment of the system, at least one camera, ideally an IP camera, is provided. This IP camera performs additional processing steps to the captured video; specifically the captured video is digitized, compressed into a convenient compressed file format, and sent to a network protocol stack for subsequent conveyance over a local or wide area network. Typical compression schemes include MPEG, JPEG, H.261 or H.263, wavelet, or a variety of proprietary compression schemes. A typical network topology is the popular Ethernet standard, IEEE 802.3, and may operate at speeds from 10 Mb/s to 100 Mb/s. Network protocols are typically TCP/IP, UDP/IP, and may be Unicast or Multicast as dictated by the system requirements.

[20] The compressed digital video is transported via Local Area Network (LAN) or Wide Area Network (WAN) to a processor which performs the steps of Facial Separation, Facial Signature Generation, and Facial Database Lookup.

[21] The utility of the system may be enhanced by the increased use of the networking techniques of the subject invention. In this enhancement, a group of networked

processors perform the steps of Facial Separation and Facial Signature generation. The Facial Processors function as network resources, and are configured to process video from any networked camera, as required. This improves the flexibility and economics of the system. For example, during periods when a particular area is not used, Facial Processors may be diverted from analysis of that particular camera to an area of higher traffic. Also, the workload of a failed Facial Processor may be diverted to a different processor.

[22] Other benefits arise from this configuration. For example, the Facial Database may be treated as a general-purpose network resource, allowing a greater number of cameras and Facial Processors to perform Facial Signature lookups at any given time. Moreover, the digital IP surveillance network is often part of a larger "network of networks", thus allowing the Facial Database to be consulted by devices on a different network. This is useful in cases where different organizations may have compiled different Facial Databases. For example, an airport may maintain a database of the Facial Signatures of all current employees, as well as of past employees. A law enforcement organization may maintain a separate database of known offenders, and an Intelligence organization may maintain a current database of foreign nationals of interest. In the depicted networked environment, the Facial Processors may consult several different Facial Databases, across the LAN or WAN.

[23] An additional benefit arises from the fact that IP surveillance systems often maintain an archive of stored video or images. Since this archive is generally available on the network, it is possible to use the system to search for faces in archived images, during event reconstruction. In the preferred embodiment the IP surveillance network

stores captured images or video in an Image Database. Often, these images are captured only when the associated camera has detected motion within its field-of-view, thus reducing the storage requirements of the image archive platform. Since the Image Database is a generally-available network resource, it is thus possible to perform the Facial Processing on these stored images as well as on live camera video.

[24] For example, the Facial Processors and Facial Database detect the presence of a person of interest in some live scene. Using the image archive, it is possible to track the person's movements backward in time, thus re-constructing the person's movements through a facility. It is additionally possible, for example, to note whether the person-of-interest may have made contact with other people within the area being monitored. The system may then, upon command, derive a Facial Signature from that 'new' person's image, and add that new Facial Signature to the Facial Database. Historical analysis of the 'new' person's movements through the facility may then be performed, or the real-time location and movements of the 'new' person may be tracked.

[25] The Facial Database and the Image Archive may be two distinct platforms, both resident on the LAN or WAN, or where desired both functions may be resident on the same physical platform.

[26] In a further enhancement of the invention, the IP cameras include additional processing resources, and are thereby capable of performing the Facial Processing internally. The separate Facial Processors of the previous example are thereby eliminated. This approach allows improvement of the storage efficiency of the Image Database since images may, if desired, only be stored in the Image Archive if a face is

recognized by one of the cameras, or if a particular predetermined face is detected by the Facial Database.

[27] My previous applications and patents as listed above and as incorporated by reference herein describe a surveillance system wherein the IP cameras may produce multiple video streams as the system requirements may dictate. For example, the IP cameras may produce several motion MPEG video streams with different bandwidths (for different audiences), and may additionally produce a high-resolution still frame JPEG image for storage in an image database. The system may utilize any of these video streams for facial recognition. Since the cameras are IP-based, their motion video and still frame video streams are generally available upon demand throughout the network, and either type of video may be used to drive the Facial Recognition system. The still frame images have the advantage of greater resolution, but may be generated less frequently. Motion video sources may produce useful images more often, but at a reduced resolution. This reduced resolution decreases the accuracy of the Facial Recognition process.

[28] Prior disclosures have additionally described the use of Multicast protocols to support the one-camera-to-many-viewers nature of the surveillance system without duplicating network traffic. This Multicast network protocol lends itself well to the present invention. Specifically, the Facial Processor is another 'viewer' on the network and no additional network traffic need be generated for it. Previous disclosures have described the use of Multicast protocol to convey the motion video, and Unicast protocols to convey the still-frame images to the image database. In the present invention, the still-

frame images may also be conveyed over the network as Multicast data, since there is more than one recipient of the still images.

[29] The subject invention is directed to the overall integration of the Facial Recognition technology with the IP camera network. IP cameras produce a variety of real-time data streams. Motion video may be compressed into two simultaneous transport streams, such as a low-resolution QSIF stream and a higher-resolution SIF stream. (SIF is normally 352x288 resolution, and QSIF is normally 176x144 resolution.) Audio may be captured, digitized into a low-bit-rate stream for transport over the network. In addition, the still-frame images may be captured at a high resolution, say 704x480, and compressed into image files sufficiently small as to meet system requirements. As previously described, these still-frame compressed image files may be conveyed by the network as a Multicast stream, or as a pair of Unicast streams.

[30] Monitor stations are configured to display the scenes captured by one or more of the networked video cameras. The monitor station may display one or multiple cameras. To conserve system bandwidth and the monitor station processing capacity, larger arrays display the low-resolution QSIF streams, while the single-camera array displays the selected camera's SIF output. The system also supports wireless monitor stations, typically used by guards or other law enforcement personnel who require mobility.

[31] An image server receives and stores still-frame images produced by the cameras for subsequent retrieval and analysis. These still-frame images are ordinarily produced only when the associated camera has detected motion within its field-of-view. The server may additionally be configured to store motion video streams upon detection of motion within its field-of-view. A facial database processor contains a stored database of the

Facial Signatures and associated "mugshots" of some previously-defined persons. A facial processor detects faces within a selected camera's captured video, and subsequently derives unique Facial Signatures from the detected faces. Facial Signatures thus detected are forwarded to the Facial Database for correlation with a previously stored 'library' of facial mugshots, associated Facial Signatures, and database images in which the current Facial Signature was previously detected.

[32] In one configuration of the invention an Image Database stores captured still images from the various IP cameras within the network. Each captured image is stored in some predetermined location within the server's file system. Each such image is represented by a unique Image ID number, maintained in a database file. Within the file, each record contains the Image ID number, as well as related data such as the date and time the image was taken, physical location where the image was taken, which camera captured the image, a fully-qualified URL describing where the image is located, and any Facial Signatures which were detected within the image.

[33] In a typical structure for the Facial Signature Database, each unique Facial Signature file contains the Facial Signature data, the subject's name if known, age, weight, aliases if any, URL of a mugshot or separated facial image, URL of a biographical file if any, and image ID numbers of any Image Database records which contain the current Facial Signature.

[34] There are several primary objectives of the invention, directed to the following activities: (1) identifying and looking for suspicious person; (2) providing access control; (3) attendance taking and verification; (4) identification and verification of friend or foe; (5) automated signaling upon verification of an issue; (6) management and distribution of

the data; and (7) interconnectivity with other facial recognition databases and with other surveillance systems and equipment.

[35] It is, therefore, an object and feature of the invention to integrate facial recognition technology with other surveillance technology for defining an enhanced multi-media surveillance capability.

[36] It is also an object and feature of the subject invention to provide improved facial recognition capability by utilizing high resolution digital camera technology to capture the image.

[37] It is another object and feature of the subject invention to provide interconnectivity between facial recognition systems and other surveillance systems.

[38] It is an object and feature of the subject invention to provide an IP network capability for transmitting facial recognition data using IP protocol.

[39] It is a further object and feature of the subject invention to provide off network connectivity of the facial recognition database to other database system including national archives and the like.

[40] It is another object of the invention to provide management and distribution of facial recognition data.

[41] Other objects and features of the invention will be readily apparent from the accompanying drawings and detailed description of the preferred embodiment.

Brief Description of the Drawings

Fig. 1 (Prior Art) is a view of prior art facial recognition systems.

Fig. 2 depicts the application of the basic Facial Recognition technology to a networked surveillance system.

Fig. 3 is an expansion of the system of Fig. 2 showing the IP cameras with additional processing resources capable of performing the Facial Processing internally.

Fig. 4 includes IP cameras for producing several motion MPEG video streams with different bandwidths, and additionally a high-resolution still frame JPEG image for storage in an image database.

Fig. 5 depicts a typical structure for an Image Database and a Facial Signature Database.

Fig. 6 depicts a typical screen layout of such a Monitor Station.

Fig. 7 depicts the overall network.

Fig. 8 depicts an expanded network for an airport system.

Fig. 9 depicts typical apparatus used at curbside check-in for an airport system.

Fig. 10 depicts a typical arrangement at a ticket counter of an airport system.

Fig. 11 depicts the equipment at a typical entry point for checked baggage, such as at the ticket counter.

Fig. 12 depicts the equipment at a typical security checkpoint used for passenger screening.

Fig. 13 depicts the apparatus used at a typical boarding gate.

Fig. 14 depicts an aircraft being loaded with checked baggage.

Fig. 15 depicts apparatus installed on board a mass-transit vehicle, herein depicted as an aircraft.

Detailed Description of the Preferred Embodiments

[42] The subject invention provides both the method and apparatus for incorporating facial recognition technology into a comprehensive, multi-media surveillance system

capable of: (1) identifying and looking for suspicious person; (2) providing access control; (3) attendance taking and verification; (4) identification and verification of friend or foe; (5) automated signaling upon verification of an issue; (6) management and distribution of the data; and (7) interconnectivity with other facial recognition databases and with other surveillance systems and equipment.

[43] The suspect finding and identification methodology includes:

- Running the Facial Recognition on the camera data;
- Running the Facial Recognition Algorithms on the Archival Database;
- Generating and storing a Facial Signature for each person that was in the field of view for future analysis;
- Automatic indexing into the Database based on signature;
- When a Suspect match has occurred, dispatch an event alarm to a wire monitor station;
- When a Suspect Match has occurred, dispatch an event alarm to a wireless monitor station, such as in a police car or a unit carried by an officer; and
- When a Suspect Match has occurred, dispatch and event alarm by telephone, cellular telephone, by pager, by digital pager, by e-mail such as through a security notification system.

[44] The access control function includes:

- Integrating the Facial Recognition with an access control database. Store the signature and the access allowed/denied;
- Notification on the access denied utilizing the notification system; and
- Access / No Access can be shown on monitors station(s).

[45] The automated attendance function includes:

- Example - an employee reports to work. The camera detects her/him entering and the employee is logged in. The camera (or another camera) detects her/him leaving and the employee is logged out. This can be automatic, or can be in conjunction with pushing an in/out interface device.
- Example – in a school a student enters a room through a door that is surveilled by a camera. As he/she enters, the student is identified and counted in attendance. Time can be part of the equation. If the student is late to class by a few minutes, the student will be counted tardy and the amount of time late recorded. If the student comes very late, attendance will not be recorded.
- A camera covering the entire room can also be utilized. The camera will have a view of all seats in the classroom. A "video roll call" of the classroom will be taken in a manner similar to the above.

[46] The identification of friend or foe function includes:

- Faceprints of known individuals, such as employees or contract personnel, would be placed in a database.
- Areas that are accessible by each person could also be put in the database.
- If an UNKNOWN person is identified in a field of view, and alarm condition is generated.
- The video is automatically switched at a monitor station and the unknown individual is flagged, such as by a circle or pointer,

- The video of the unknown individual would be flagged, such as by a circle or pointer, and tracked as he/she moved around.
- If a known (or unknown) person is in a field of view, the time and location is logged on a database.
- If it is desired to know where a particular person has been and what they are doing there, the database can be polled and the associated images or video immediately brought up for review.
- If a known individual enters an area that is not accessible by that individual, an alarm condition can be generated.
- The alarm condition can:
    - Generate an audible alarm at the area of infringement.
    - Generate an alarm at a monitor station.
    - Switch the video to the monitor station.
    - Start video tracking of the individual.
    - Log the video to a server.
    - Log the locations pursued to the server.
    - Log the time for each of the locations.
- Example – in a school, if a student is supposed to be in a particular classroom at a particular time, if he is found in other areas an alarm event can be generated.
- The system can log all areas that an individual visits.
- The system can show individuals on a map:
    - By an Icon

- By Name
- By a small photo of their face
- By Function (nurse, doctor, security, maintenance, student, Freshman, Senior, Teacher, Coach, Administration, Security, etc.).
- By Department (Maintenance, Library, Engineering, etc.).
- Clicking on the icon on the map for each person can give more data if it is not presented on the map display:
  - Name
  - ID Number
  - Department
  - Rank
  - Student schedule

SYSTEM ARCHITECTURE

[47] Figure 1 depicts prior-art Facial Recognition systems. In Prior Art #1, video camera 1 views a scene of interest, and processor 2 analyzes the video signals produced by the camera. The processor performs the steps of:

- Facial Separation, e.g., locating human faces within the viewed scene,
- Facial Signature generation, e.g., deriving a unique identifying descriptor for the detected faces,
- Database Creation, adding said descriptors and separated facial image to a comparison database,
- Database Lookup, matching the captured descriptors with previously-captured faces or images containing faces or other relevant data, and

- Generating alarms as appropriate.

[48] In Figure 1, the basic function of the system can be enhanced as depicted in Prior Art #2. As shown, the processing function has been divided among several processors. One or more processors 3 perform the computationally intensive tasks of Facial Separation and Facial Signature generation, while processor 5 performs the less demanding task of database pattern matching. This yields improved system economies and flexibility: cameras and Facial Processors may be added incrementally to the system as needed, and it is unnecessary for each Facial Processor to contain or to access the entire 'reference' database.

[49] Figure 2 depicts the application of the basic Facial Recognition technology to a networked surveillance system. Important aspects and features of the system and described in detail herein are the following:

- IP Video Cameras Driving Facial Recognition.
- Networked IP Video Cameras Driving Facial Recognition.
- IP Video Cameras Driving Networked Recognition.
- Networked IP Video Cameras driving both Image Database and Network Recognition.
- Use of MPEG I-Frames from Stream to drive Recognizer.
- Use of High-Resolution Still Streams to drive Recognizer.
- Use of Multicast to send Motion Streams to Monitor and Recognizer simultaneously.
- Use of Multicast to send Still Streams to Monitor and Recognizer simultaneously.

- Tagging of archived images in the database, where faces have been located on that image, with the all of the "facial signatures" of individuals seen in that image. Note that these signatures may be of known or of then unknown persons. This can be done in real-time or post processed.

[50] In the system of Figure 2, and labeled "IP #1", Camera 20 is an "IP camera", as distinct from the conventional analog camera in the prior art. This IP camera perform additional processing steps to the captured video; specifically the captured video is digitized, compressed into a convenient compressed file format, and sent to a network protocol stack for subsequent conveyance over a local- or wide area network. Typical compression schemes include MPEG, JPEG, H.261 or H.263, wavelet, or a variety of proprietary compression schemes. A typical network topology is the popular Ethernet standard, IEEE 802.3, and may operate at speeds from 10 Mb/s to 100 Mb/s. Network protocols are typically TCP/IP, UDP/IP, and may be Unicast or Multicast as dictated by the system requirements.

[51] The cameras' compressed digital video is transported via Local Area Network (LAN) or Wide Area Network (WAN) 21 to a processor 22 which performs the steps of Facial Separation, Facial Signature Generation, and Facial Database Lookup.

[52] The utility of the system may be enhanced by the increased use of modern networking techniques, as Figure 2 depicts in diagram "IP #2". In this enhancement, a group of networked processors 25 perform the steps of Facial Separation and Facial Signature generation. This is distinct from the network topology of Figure 1, in which specific Facial Processors are dedicated to specific cameras. In Figure 2, the Facial Processors 25 are treated as network resources, and are configured to process video from

any networked camera as required. This improves the flexibility and economics of the system. For example, during periods when a particular area is not used, Facial Processors may be diverted from analysis of that particular camera to an area of higher traffic. Also, the workload of a failed Facial Processor may be diverted to a different processor.

[53] Other benefits arise from the topology of Figure 2. For example, the Facial Database 24 may be treated as a general-purpose network resource, allowing a greater number of cameras 20 and Facial Processors 25 to perform Facial Signature lookups at any given time. Moreover, the digital IP surveillance network is often part of a larger "network of networks", thus allowing the Facial Database to be consulted by devices on a different network. This is useful in cases where different organizations may have compiled different Facial Databases. For example, an airport may maintain a database of the Facial Signatures of all current employees, as well as of past employees. A law enforcement organization may maintain a separate database of known offenders, and an Intelligence organization may maintain a current database of foreign nationals of interest. In the depicted networked environment, the Facial Processors 25 may consult several different Facial Databases, across the LAN or WAN.

[54] An additional benefit of this topology arises from the fact that IP surveillance systems often maintain an archive 23 of stored video or images. Since this archive is generally available on the network, it is possible to use the system to search for faces in archived images, during event reconstruction. For example, the IP surveillance network of Figure 2 stores captured images or video in an Image Database 23. Often, these images are captured only when the associated camera has detected motion within its field-of-view, thus reducing the storage requirements of the image archive platform.

Since the Image Database 23 is a generally-available network resource, it is thus possible to perform the Facial Processing on these stored images as well as on live camera video.

[55] For example, the Facial Processors 25 and Facial Database 24 detect the presence of a person of interest in some live scene. Using the image archive, it is possible to track the person's movements backward in time, thus re-constructing the person's movements through a facility. It is additionally possible, for example, to note whether the person-of-interest may have made contact with other people within the area being monitored. The system may then, upon command, derive a Facial Signature from that 'new' person's image, and add that new Facial Signature to the Facial Database. Historical analysis of the 'new' person's movements through the facility may then be performed, or the real-time location and movements of the 'new' person may be tracked.

[56] Figure 2 depicts the Facial Database and the Image Archive as two distinct platforms, both resident on the LAN or WAN. It should be noted that these functions are essentially software, hence both functions may be resident on the same physical platform if system requirements so dictate.

[57] Figure 3 depicts a further extension of the invention of Figure 2. In Figure 3, the IP cameras 30 have been enhanced with additional processing resources, and are capable of performing the Facial Processing internally. The separate Facial Processors of the previous example are eliminated. In addition, this approach allows improvement of the storage efficiency of the Image Database 34, since images may, if desired, only be stored in the Image Archive if a face is recognized by one of the cameras 30, or if a particular predetermined face is detected by Facial Database 33.

[58] The previously listed and incorporated applications and patents have described a surveillance system wherein the IP cameras may produce multiple video streams as the system requirements may dictate. For example, in Figure 4 the IP cameras 40 may produce several motion MPEG video streams with different bandwidths (for different audiences), and may additionally produce a high-resolution still frame JPEG image for storage in an image database 45. Note that the system of Figure 2 may utilize any of these video streams for facial recognition. Since the cameras 40 are IP-based, their motion video and still frame video streams are generally available upon demand throughout the network, and either type of video may be used to drive the Facial Recognition system. The still frame images have the advantage of greater resolution, but may be generated less frequently. Motion video sources may produce useful images more often, but at a reduced resolution. This reduced resolution decreases the accuracy of the Facial Recognition process.

[59] The previously listed patents and applications also describe the use of Multicast protocols to support the one-camera-to-many-viewers nature of the surveillance system without duplicating network traffic. This Multicast network protocol lends itself well to the present invention. The Facial Processor is simply another 'viewer' on the network and no additional network traffic need be generated for it. Multicast protocol is used to convey the motion video, and Unicast protocols to convey the still-frame images to the image database. In the present invention, the still-frame images may also be conveyed over the network as Multicast data, since there is more than one recipient of the still images.

[60] Figure 4 depicts the overall integration of the Facial Recognition technology with the IP camera network. IP cameras 40 produce a variety of real-time data streams as shown. Motion video may be compressed into two simultaneous transport streams, such as a low-resolution QSIF stream and a higher-resolution SIF stream. SIF is normally 352x288 resolution, and QSIF is normally 176x144 resolution. Audio may be captured, digitized into a low-bit-rate stream for transport over the network. In addition, the still-frame images may be captured at a high resolution, say 704x480, and compressed into image files sufficiently small as to meet system requirements. These still-frame compressed image files may, as previously described, be conveyed by the network 47 as a Multicast stream, or as a pair of Unicast streams.

[61] Figure 4 also depicts the remainder of the surveillance network. Monitor stations 41 and 44 are configured to display the scenes captured by one or more of the networked video cameras 40. The monitor station may display one camera, or may display four cameras in a 2x2 array, nine cameras in a 3x3 array, or sixteen cameras in a 4x4 array. To conserve system bandwidth and the monitor station's processing capacity, larger arrays such as 4x4 display the low-resolution QSIF streams, while the single-camera array displays the selected camera's SIF output.

[62] Figure 4 additionally depicts a 'wireless' monitor station 43, which receives selected video streams from the network via Wireless Access Point 42. Due to the bandwidth constraints typical of wireless systems, a QSIF stream is normally displayed in the application. Such a wireless monitor station is typically used by guards or other law enforcement personnel who require mobility.

[63] Figure 4 also depicts an image server 45. This server receives and stores still-frame images produced by cameras 40, for subsequent retrieval and analysis. These still-frame images are ordinarily produced only when the associated camera has detected motion within its field-of-view. Server 45 may additionally be configured to store motion video streams upon detection of motion within its field-of-view.

[64] A Facial Database 47 is depicted in Figure 4. As previously described, this processor contains a stored database of the Facial Signatures and associated mugshots of some previously-defined persons.

[65] Finally, Figure 4 depicts the networked Facial Processors 46, which detect faces within selected camera's captured video, and which subsequently derive unique Facial Signatures from the detected faces. Facial Signatures thus detected are forwarded to the Facial Database 47 for correlation with a previously stored 'library' of facial mugshots, associated Facial Signatures, and database images in which the current Facial Signature was previously detected.

[66] Figure 5 depicts a typical structure for an Image Database and a Facial Signature Database. The Image Database stores captured still images from the various IP cameras within the network. Each captured image is stored in some predetermined location within the server's file system. Each such image is represented by a unique Image ID number, maintained in a database file. Within the file, each record contains the Image ID number, as well as related data such as the date and time the image was taken, physical location where the image was taken, which camera captured the image, a fully-qualified URL describing where the image is located, and any facial Signatures which were detected within the image.

[67] In a typical structure for the Facial Signature Database, each unique Facial Signature file contains the Facial Signature data, the subject's name if known, age, weight, aliases if any, URL of a mugs hot or separated facial image, URL of a biographical file if any, and image ID numbers of any Image Database records which contain the current Facial Signature.

[68] Previous Figures have depicted the presence of a networked Monitor Station. A typical screen layout of such a Monitor Station is depicted graphically in Figure 6. A Map Pane 61 contains a map of the facility under surveillance. This Map Pane may contain multiple maps, possibly representing different floors or buildings within a facility. Different maps may be displayed through common 'point and click' methods. Each map contains graphical icons representing the location and ID's of the various IP cameras available on the network. Video Pane 62 contains the current video of the selected camera or cameras. When viewing stored images from the Image Database, this Video Pane displays selected images from the database. A Control Pane 63 presents a variety of context-sensitive GUI User controls.

SUSPECT IDENTIFICATION AND ALARM TECHNIQUES

[69] With the Facial Processors and the Facial Database available on the LAN or WAN, a number of useful and novel applications become possible.

[70] Within a facility, the various IP cameras view scenes of interest, and one or more Monitor Stations display video from a selected group of cameras. Facial Processors locate faces in video from selected cameras, and derive Facial Signatures from the detected faces. These Facial Signatures are transmitted to a Facial Database, which searches through its stored Facial Signature library for a match.

[71] When the Facial Database scores a 'hit', it forwards appropriate information to the networked Image Database server. This information includes:

- The camera ID and image ID in which the match was found
- The location within the image where the matching face is located
- The stored Facial Signature which matched
- The stored mugshot associated with the Facial Signature
- Related information associated with the Facial Database record, such as the person's name, age, employer, criminal history, etc.

[72] Upon receipt of this data, the Image Database server may perform the following steps:

- The server appends the descriptive information from the Facial Database to the current image that contained the hit.
- The server forwards the 'hit' information to all Monitor Stations on the network. The Monitor Stations thereupon bring the current image, containing the Facial Match, to the forefront of the application screen.
- Monitor stations additionally display the matching face from the database, plus other descriptive information provided by the database.
- The 'hit' event is added to the system log.
- The server likewise alerts any mobile or wireless Monitor Stations of the presence of the 'hit' and it's location.
- The server forwards the matching face and related descriptive information from the Facial Database to the wireless Monitor Station for display.

- The server alerts appropriate personnel from a predetermined list, using e-mail, pagers, or an automated telephone message.
- The server may additionally send a message to an associated facility security system, which thereupon locks entry doors as appropriate.

PERSONNEL LOCATION AND TRACKING

[73] When the system is enhanced with Facial Recognition technology, a number of useful and novel functions may be added to the basic surveillance system. The basic functions are as follows:

- "Hit" is automatically located on map. Map is brought forward automatically if required.
- A moving "Hit" is tracked on the map.
- "Where is" our person - Locating individual personnel by query, such as security guard or maintenance personnel. Key in query, response is location, map location, and/or video of his location.
- "Where is" Security Guard tracking and logging of locations present and time of presence in database.
- Alarm condition if guard is not seen at specified location during rounds by predetermined time.
- "Where is" Lost Child implementation – local scanner input of photo, activate recognition function.
- Automatic tracking of manually "Tagged" personnel of interest– searches forward in real time, backwards in database. Graphical User Interface for "Tagging" suspect of interest.

- Use of Image Database – find an unknown suspicious person or person perpetrating an event and "cut" their facial image, reduced it to its signature, then do "find".
- The "find" above can be done in real-time to find the person at the present time in the facility.
- In real-time, if not found, set "trap" to add to APB (define) list for future ID. Upon finding individual, alarm event is notified, and attached notes as to incident and images can be brought into focus.
- The "find" above, can be done against the database, either an image or a signature database, to find other instances that the individual was on premises, and see what he was doing.
- The "find" can either look against stored facial signatures, or against stored raw images that are analyzed during post-processing.

[74] When the Facial Database detects a 'hit', the location of the hit is depicted on map pane 61 of Figure 6. The appropriate map may be brought forward, if not already displayed, and the associated camera icon is highlighted, flashed, or otherwise made visually distinct. The subject person's current location within the facility is thus displayed. As subsequent hits are detected, possibly at a succession of cameras if the person is in motion, the associated camera icon is again highlighted, indicating the person's movements.

[75] Inquiries regarding the current location of individual personnel may be performed by the system. As an example, a previously-enrolled person is selected from the Facial Database, using the person's name, mugshot, employee ID, or other stored information.

This selection may be made from a Graphical Interface on a networked Monitor Station. The Facial Database is then instructed to look for a 'hit' on that record. When one of the networked IP cameras captures an image, subsequently determined by a networked Facial Processor to contain that person's face, the Facial Database informs the Monitor Station of the match. The Monitor station may then highlight the camera icon of the associated camera, effectively locating the desired person on the map. The Monitor station may additionally bring that camera's video to the forefront, displaying a current image of the desired person.

[76] In an enhancement of this application, the desired person's movements may be compared against a known route, schedule, or database of approved/ restricted locations. For example, a security guard may have a predefined route to cover, which defines locations and times of his rounds. The Facial Database may be instructed to look through real-time images for a match with this person. If any such matches are found, they are compared with the times and locations defined by the guard's predefined schedule. If the guard successfully follows his usual rounds, the Facial Database can log this in a security log, including times and locations of the guards' route. If, however, the guard is not detected at the predefined location and/or time, this fact may be logged and, optionally, a system alarm may be generated to notify appropriate security personnel. Additionally, it is possible for the system to detect any non-approved persons in those areas, and generate an alarm. For example, a night guard may have a predefined set of rounds to cover. The system may detect the presence of the guard at the correct times and locations, and note this in a log file. Detection of the guard would not cause a system alarm, however, the detection of any other personnel at those times and places would generate an alarm.

Likewise, detection of that guard at an unexpected location or place would generate an alarm. Note that it is not necessary for said 'other' personnel to have been previously enrolled in the database; the mere detection of any Facial Signature other than that of the predefined guard would generate a system alarm.

[77] In a Hotel application, hotel guests may be enrolled into the system at the time of registration. Hotel employees may likewise be enrolled into the system at the time of their employment. The system may be instructed to log the time and location of each successful facial detection, whether a database 'hit' occurs or not. If the facial detection does not match any person enrolled in the Facial Database, the system may generate an alarm, and indicate on a networked Monitor Station the location, and live video, where the face was detected. By way of example, common hotel burglars are thereby automatically detected and recorded by the system, and the system can be instructed to generate an alarm upon the next occurrence of this person. On the other hand, if the detected face is enrolled in the Facial Database, the system may determine what action to take based upon a pre-defined set of rules. For example, if a previously-enrolled guest is detected on the correct floor, then the event is logged but no alarm is generated. If the guest is detected on the wrong floor, the event is logged and an alarm may or may not be generated based on a pre-defined qualifier. An employee may be detected, and an alarm may or may not be generated based on the employee's schedule or authorizations. For example, a cleaning lady on the correct floor at the correct time would not generate an alarm, but the same person on the wrong floor may generate an alarm.

[78] In an airport security application, all persons who successfully pass through a security checkpoint are photographed and enrolled into a networked Facial Database. In

addition, the person's itinerary is recorded into the database. This Facial Database may then be shared among several airports. Thus, in any airport:

- Detected faces that do not match any Facial Database entry may generate an alarm, directing security personnel to the location of the 'unknown' person, and may cause a suitable networked monitoring Station to display the real-time video.
- Detected faces that match an approved passenger in the Facial Database may be compared with the person's itinerary for that trip. If the passenger is in some location or airport that does not match the passenger's itinerary, then security personnel may be alerted to the person and to their location.
- Personnel who attempt to board an aircraft without having been enrolled into the Facial Database may generate an alarm, and may be detained by security personnel.
- Airport employees who may be in unauthorized areas, or who may attempt to approach or board an aircraft, may generate an alarm to appropriate security personnel.

[79] In a useful enhancement of this application, a previously unknown person may be 'enrolled' into the Facial Database, and a facility-wide search may be commenced. A lost child, for example, may be enrolled into the system through the use of a photograph scanned into the Facial Database. In lieu of a photograph, all children entering some facility, such as an airport or theme park, may be photographed and enrolled into the Facial Database. The Facial Database may then search all real-time camera video for a

match with the enrolled child. When a networked IP camera produces video which is subsequently determined to contain the lost child's face, one or more networked Monitor Stations alert security personnel of the event, and provide location and camera video of the lost child. Security personnel may then be dispatched to the location of the child.

[80] Other applications of personnel tracking may require that a person be manually 'enrolled' into the Facial Database. For example, a person seen in a live image may be 'tagged' by an operator at a Monitor Station, whereupon the 'tagged' person's Facial Signature is added to the Facial Database. This is accomplished through the use of a GUI, wherein a specific still-frame image (or a frozen frame from a moving image) is displayed to the Monitor Station operator. The operator selects the desired face from the displayed image, through the use of a mouse or equivalent pointing device. The selected face is then separated from the image, the Facial Signature is derived, and the Facial Signature is added to the Facial Database. The operator is prompted to provide other pertinent information as appropriate to the application, such as a description of the observed event.

[81] The Facial Database may then be instructed to flag an operator whenever the 'tagged' person's image appears in any of the real-time images captured by the networked IP cameras. If the 'tagged' person's face is not observed by the Facial Database within some predefined time interval, then the Facial Database may be instructed to add the person's Facial Signature to a 'watch list' within the Facial Database. If the person's Facial Signature is subsequently detected by the Facial Database, then an alarm is generated, and selected Monitor Stations 'pop' the relevant information onto the Monitor Screen.

[82] Alternatively, the Facial Database may be instructed to search through the Image Database for all occurrences of the 'tagged' person's Facial Signature. This search may be made against the Image Database, or against the Facial Signature database, which keeps a record of all image filenames in which the selected Facial Signature occurs.

LAW ENFORCEMENT

[83] The invention has applications in day-to-day law enforcement:

- Police car has on-board suspect database or link to database. When an officer stops a suspect, lookup occurs.
- A policeman sees a suspicious person, it is logged into a database along with notes from the officer. That information is then disseminated to other officers using facial key. If that suspect is encountered again by the same or a different officer, previously collected information will be available.

[84] The surveillance network may include the use of wireless, mobile Monitor Stations as well as the use of wireless IP cameras, all of which are part of the overall IP surveillance network. A patrol officers squad car may be equipped with both a wireless IP surveillance camera, as well as a wireless Monitor Station. When an officer stops a suspect, the suspect's image may be captured by the car's wireless surveillance camera. The captured image may then be forwarded to a networked Facial Processor, which derives a Facial Signature from the suspect's image. This Facial Signature may be forwarded to the Facial Database, which looks for a match between the suspect's Facial Signature and any Facial Signatures which may have been previously recorded. Thus, Suspects may be quickly and accurately identified during the stop.

[85] In another application, a suspicious person's image is captured by a wireless IP surveillance camera, and the Facial Signature is generated as before. The Facial Signature is stored in the Facial Signature database, along with other information collected by the officer, such as location, time, type of activity observed, and so on. This information is then available to other officers via the Facial Signature database. If another officer encounters the person, the person's image may be again captured, and the ensuing Facial Signature match may alert the officers as to the previous suspicious activity. In this way, a person's behavioral pattern may be easily and systematically detected and recorded, such as a person who may be 'casing' a bank prior to a potential robbery.

ATTENDANCE LOGGING

[86] The surveillance network, as supplemented with the Facial Recognition technology, finds usefulness in daily attendance applications:

- Students logged in to class and time stamped. By comparison to schedule database, create Automatic Absentee and Tardy logging and notification.
- Automatic correlation of absent and tardy people that are found in other areas. Alarm conditions can be generated, video selected on monitor stations, icons brought up on maps.

[87] For example, an IP camera may be trained at a classroom doorway, so as to capture facial images of attendees. Alternatively, the camera may be positioned to view the entire room. In either case, the images thus collected may be used to find faces, derive Facial Signatures, and compare a list of persons present to a class schedule

database. This effectively automates the process of attendance taking. The system may thus record attendees, plus absentee or tardy students.

[88] The system may additionally correlate the real-time list of tardy or absent students against Facial Signatures of students detected in other areas of the school. In the event of a database 'hit', the system may generate an alarm, and display the surveillance image of the student. The Monitor Station may additionally display relevant student information, such as name, current location, classroom where the student is scheduled to be, or prior attendance information.

SECURE AREA PATROL

[89] In secure areas where access by authorized personnel is strictly controlled, the system has important applicability both in monitoring and in controlling access. Features include:

- Known personnel approved for specific area access are not alarm events if seen. All others are alarm events.
- Known personnel approved for specific area access at specific times and dates are not alarm events if seen. All other personnel are alarm events, or known personnel outside of approved area at approved time are alarm events.
- Hotel Example: Registered guests and hotel personnel logged into database. Tracking of areas covered logged, but not alarmed. All others tracked and alarmed. Time and area qualifiers also may be used, such as a guest on the wrong floor.

- Multi-Level Alarms, such as a registered guest on the right floor would be a condition green, on a wrong floor would be a condition yellow, a fired employee any place in the building would be a condition red.
- Airport/Transportation application: A problem is people in airports skipping or passing security in smaller airports where security is minimal, then flying to a major airport and having full access to flights (connections) without further security checks. The present invention addresses this by capturing an image of every person who is security checked at any facility. Their facial signature is then added to the "OK" list for that day, or for that specific itinerary and time frame. The facial signature can then be forwarded to other airports. In those airports, if any individual appears behind the security check area who has not been properly cleared by security, then an alarm is generated so that individual can be investigated. Personnel, such as airport employees, who try to board planes without being passengers or passing through appropriate security can also be apprehended by use of cameras monitoring boarding.

PANIC BUTTON INTEGRATION

[90] My previously mentioned applications and patents describe a personal 'Panic Button', to be used by teachers or other personnel who may need to alert security personnel during an emergency. The addition of Facial Recognition technology to the networked surveillance system, also previously described, enhances the utility of the Panic Button.

[91] Personnel carry a radio transmitter with a button. When an event button is pushed, the transmitter relays to a receiver that relays to the network the type of event (security request, medical request, fire request, etc.) and the individual who generated the event. The facial recognition system would then look for the last known location of that individual, and identify the event in that area – such as map indication, camera selection, and response personnel dispatch.

[92] In an example application, the panic button transmitter may contain one or more pushbuttons labeled, for example, 'FIRE', 'MEDIC', "POLICE' and so on. When the user presses a button, an internal processor composes a message which encodes the identity of the person and the nature of the emergency (as derived from which button was pressed). This message is then transmitted to one or more networked receivers, and is displayed on one or more Monitor Stations. Security personnel may then be dispatched to the person's location as required.

[93] It is often difficult to determine, with any accuracy, the exact location of the person who signaled the emergency. With RF-based systems, the location of the transmitter may only be determined to within the working radius of the receiver(s) that detected the transmission. Typically, such receivers have a fairly broad coverage area, so as to minimize the total number of receivers required to completely cover the facility. Thus, localization of the person sending the alarm is of poor accuracy.

[94] With the addition of Facial Recognition technology to the network, this problem is solved. When a networked Panic Button receiver detects a transmission from a known person, the Facial Database looks up the person's Facial Signature, and proceeds to search all incoming video for a match. This localizes the person to within the field of

view of one particular camera. The system additionally displays the current video from that camera.

[95] Moreover, if the Facial Database fails to detect the person's Facial Signature in any current video, then the Facial Database may be instructed to search the Image Database for the person's image. Such a search would start at the most recently stored images, preferably starting with previously known locations, if any, where the person was scheduled to have been. When a match is detected, the Monitor Station may be instructed to display the most recent image containing the person's image.

INTELLIGENT RESPONSE DISPATCH

[96] Certain types of security alarm events may require the dispatch of specific types of personnel:

- Events that require response, such as fire alarms, alarm system triggers, facial recognition "hits" on suspects can be geo-located by some means, such as fixed sensors at known locations, or facial recognition events. When the location of such an event is determined by the system, the location of appropriate response personnel based on last known facial recognition can be utilized. For example, if a "security" panic button is pushed and location determined, the closest security guard to the area of the alarm as determined by the facial recognition system can be dispatched.
- Use of Access Point determination communication links to a mobile guard station will identify area that the guard is in. Dispatch of closes response person can then be accomplished.

[97] For example, a fire alarm might require the immediate dispatch of firefighters, while a medical alarm might require the immediate dispatch of a nurse or doctor. A security violation at an entrance door may require the dispatch of a security guard.

[98] It may be difficult to provide such immediate personnel dispatch if the location of the various personnel is not known. Addition of Facial Recognition technology to the networked security surveillance system eases, and may indeed automate, such dispatch.

[99] In such a system, all security, fire, medical, or administrative personnel, for example, are enrolled into the Facial Database. Upon detection of a particular type of system alarm, for example a fire alarm, the Facial Database is instructed to search all incoming video for a Facial Signature match with one of a group of pre-enrolled firefighters. When the Facial Database successfully detects one or more of these firefighters, their current location is indicated on the Monitor Station. This indication may be via graphical icons on the facility map, or by displaying the camera(s) which contain their video. In either case, the available firefighters are located, and the nearest ones can be dispatched to the scene of the fire.

AD HOC DATABASE ACCUMULATION

[100] Previous examples have mostly involved the use of a pre-defined database of Facial Signatures. Other applications of the system may involve the use of a Facial Database that is collected over a period of time.

[101] Databases of individuals can be built-up automatically. Link of the surveillance system, with other systems such as ATMs, ticketing systems, and the like can be made. As an individual does a transaction his facial signature is logged. If another transaction is attempted but a different facial signature is involved, and alarm is generated.

[102] A person's image and Facial Signature may be collected as part of a routine transaction, and added to a Facial Database for later use. This approach has merit in transactions involving ATM's, ticketing systems, gas pumps, banking, or a variety of over-the-counter purchase transactions.

[103] By way of example, airline tickets are used under a specific name and a facial signature and an image are collected. If the same name is used again, but a different facial signature is seen, an alarm event is generated. The use of the previously captured image can be utilized for operator intervention to determine what has happened.

[104] Conversely, if the same facial signature shows up again in another transaction, but the name is different, an alarm event is generated and the subject investigated. The use of the previously captured image can be utilized for operator intervention to determine what has happened. This could be a terrorist attempting to travel on a stolen ID, or could be a recently married lady whose name changed. The image can verify it is the same person, investigation would have to address changing names.

[105] In another example, an ATM card or Credit Card is used. The system captures a facial signature for that specific card. An image of the user is captured and stored as well. If that card is used but a different facial signature is seen, and alarm event is generated. The use of the previously captured image can be utilized for operator intervention to determine what has happened.

[106] In yet another example, prescription drugs are purchased under a specific name and a facial signature and an image are collected. If the same name is used again, but a different facial signature is seen, and alarm event is generated. The use of the previously captured image can be utilized for operator intervention to determine what has happened.

[107] Note that in these cases, where a valid credit or ATM card is used but the Facial Signature does not match prior transactions, the Facial Database alerts other linked systems to perform a search for any transaction involving that ATM or credit card. Alternatively, the Facial Database alerts other security networks to search any available camera video for that person's Facial Signature. Thus, after a person uses a stolen ATM card at one bank, the person's Facial Signature may be forwarded to other banks in the area, which may be instructed to search for any ATM transaction, or any camera video at all which contains the selected Facial Signature.

TREND ANALYSIS

[108] An area can be monitored for repeated (suspicious) access by specific but unknown individuals. If the repeated access is over a selected threshold point, an alarm can be indicated. Images can be stored with attached facial signatures. A search of that facial signature would then bring up all images of that individual.

[109] For example, a bank can have a facial database of all current customers and bank personnel. If an unknown individual appears in the recognition system several times without becoming an employee or customer, this could create an alarm condition. A search by facial signature can go back in the database and allow investigation of what that individual was doing. If it is a known benign individual, such as the postman making mail delivery is seen, a GUI can allow "tagging" that individual from unknown to known. This would prevent generation of future alarms when that particular individual is recognized.

[110] Networked security surveillance systems such as described may use Facial Recognition methods to spot developments or trends that may be of interest. For

example, a bank's surveillance network may automatically detect and enroll all faces captured by its network of security cameras. The Facial Database may then be searched for trends, such as a new face that appears on the scene and which becomes persistent or periodic. The Facial Database may then alert security personnel to these detected patterns, via a networked Monitor Station.

[111] Most of these cases will be benign, such as the Postman or perhaps a construction crew doing renovations. An operator at a networked Monitoring Station may add an entry to the Facial Database which defines these regularly-detected Facial Signatures as 'approved', along with appropriate identifying information.

[112] Some of these cases, however, might be people reconnoitering the premises in preparation for a crime. Upon detection of such a person, security personnel may be notified via a networked Monitoring Station, and personnel may be directed to intercept the person immediately, or upon the next detection of the person. In addition, the Image Database may be searched for any occurrences of that person's Facial Signature, as part of the event analysis.

ACCESS CONTROL

[113] In this application, a networked camera captures a person at a door camera, the recognizer identifies the individual, a database lookup occurs to see if that individual is authorized for access at that time and place, access is allowed, a signal is sent to an electric door strike or other control device to allow access.

[114] In the invention, doorways are each equipped with a networked IP surveillance camera, positioned to capture the face of the person seeking entry. When a face is detected at a particular doorway camera, the Facial Database searches for a match

between the detected person's Facial Signature, and a Facial Signature in the Facial Database. If the detected person's Facial Signature is found in the Facial Database, on a list of 'approved' persons, the Facial Database commands the electric door 'strike' to open and allow the person entry to (or exit from) the facility.

CURFEW MONITORING

[115] Many locations experience problems with curfew violations, where underage persons are present at prohibited locations, or are in public locations after some predefined time. The networked surveillance system, enhanced with Facial Recognition capabilities, may be configured to automate detection of such violations.

[116] A database of affected personnel such as students or minors is created. This can be done at schools, or by means of photos on driver's licenses, for example. Cameras patrolling common street areas are deployed with facial recognition. If such people are detected in the street after curfew time, an alarm is generated and response personnel dispatched.

[117] In the invention, a number of IP cameras are positioned around some area known to be frequented by curfew violators. The networked Facial Database may be loaded with still-frame images and Facial Signatures of underage persons, perhaps from a Facial Database generated by the public schools, or from a Juvenile court, or the like. When the Facial Signature of a captured face matches a face in the Facial Database, police or other appropriate personnel may be dispatched to the location.

POINT OF SALE MONITOR

[118] The system may also be interfaced to a point of sale system, such as a gasoline pump. An image of the person activating the pump is collected. If that individual leaves

the store without paying, the facial signature and image of that individual is added to the "drive-off" list. If that individual returns to that store, the pump will be locked out and personnel can be notified of a former drive-off suspect. In addition, drive off facial signatures can be forwarded to other stations to prevent that person from accessing pumps at other locations, and assist in apprehending that person.

SHARED RETAIL "SUSPECT" SERVICES

[119] Retail establishments can collect images in conjunction with retail transactions such as use of membership cards, checks or credit cards. A facial signature of the associated image is generated. If the transaction "goes bad" the facial signature can be so noted and shared with other retail establishments. This can be within one company, it can be a cooperative service with many members, or it can be an extension of check and credit card verification services. This prevents multiple use of stolen or forged checks, credit cards, and the like.

PASSENGER & BAGGAGE TRACKING SYSTEM FOR AIR TRAVEL

[120] Figures 7 through 15 depict a comprehensive integration of the networked video surveillance system with Facial Recognition technology and with commonplace or legacy airport security measures. These airport security measures include metal detectors, baggage X-ray scanners, scales, and related devices. An integrated network of said devices improves security throughout the air travel system.

[121] Figure 7 depicts the overall network. Various airports 70 each contain a Local Area Network (LAN) to interconnect their various security equipment. Each airport is equipped, for example, with Networked Security Cameras at the curbside check-in point(s) 75, at the ticket counter(s) 76, the security screening point(s) 77, the various gate

counters 78, and at the entrance to each jetway 79. In addition, the airport facility is equipped with a group of Networked Surveillance Cameras, providing surveillance coverage of other areas of interest, including concourses, restaurants, baggage handling areas, aircraft loading areas on the tarmac, and so on. These Airport LANs are all interconnected via a national Inter-Airport WAN 71, permitting efficient dissemination and sharing of security data between airports 70 and with en-route aircraft 74 via ground station/satellite communications link 73.

[122] Figure 8 depicts the airport network in greater detail. Networked Surveillance Cameras 80A through 80E are stationed at the various security checkpoints as indicated, including curbside check-in, ticket counters, security checkpoints, gate counters, boarding gates, and so on. The Airport Security LAN contains Networked Monitoring Stations 85, Networked Facial Processors 86, Networked Image Database 87, and a Networked Facial Database 88. In addition, the Airport LAN has a connection to the National Airport Security WAN. Additional Networked Surveillance Cameras 80 are installed in various areas of interest within the airport as previously discussed. In addition to the cameras, the security checkpoints contain other Networked devices as appropriate to the function of the checkpoint. For example, at curbside check-in, scanner 81A is used to scan a departing passenger's photo ID and ticket, and thereupon store such captured information into the airport's networked Image Database. At the ticket counter, a scale 82A and explosive sensor 83 are used in screening passengers, again storing such captured information into the networked airport Image Database.

[123] Figure 9 depicts typical apparatus used at curbside check-in. Passengers 91A and 91B arrive at curbside for check-in. Networked Surveillance Cameras 90A and 90B

capture their image, for subsequent Facial Analysis and enrollment into the airports Networked Facial Database. Their baggage, 92A and 92B respectively, is additionally photographed by cameras 90A and 90B, and is weighed by a networked scale 93, and the resulting weight reading is stored in the airport's networked Image Database along with the passenger's captured Facial Signature. Additionally, the passenger's Photo ID and tickets are scanned with networked scanner 95, and the resulting images are additionally stored in the airport's networked Image Database.

[124] Figure 10 depicts a typical arrangement at a ticket counter. Passenger 103 arrives at the Ticket Counter for ticketing and baggage check. Networked Surveillance Camera 100A captures the person's image, for subsequent Facial Processing and Image storage. The passenger's baggage is weighed by networked scale 101, and the baggage is imaged by networked surveillance camera 100B. The baggage's image and weight are transferred via hub 104 to the Airport LAN, and subsequently to the networked Facial Database, and are appended to the passenger's file record in the Facial Database. Additionally, the passenger's ticket and photo ID (driver's license, passport, or the like) are scanned by networked scanner 102, and the resulting images are transferred, via the airport LAN, to the networked Image Database. Other ticket-counter scanners, such as an explosives sensor, an X-Ray scanner, or a scale 105 for weighing the passenger, likewise produce data which are appended to the passenger's record in the Facial Database.

[125] At this point, the person's Facial Signature (as derived from camera 100A's captured image) may be compared with the Facial Signature derived from the person's photo ID scan, for identity verification of the passenger. In addition, data describing the

passenger's baggage has been captured by the system and stored in the passenger's Facial Database file, for subsequent bag and identity matching.

[126] Figure 11 depicts the equipment at a typical entry point for checked baggage, such as at the ticket counter. A networked image scanner captures the passenger's photo ID, which may be a driver's license or a passport. Camera 111A captures an image of the passenger and baggage at that time, and the ensuing Facial Signature may be confirmed against the Facial Signature derived from the passenger's photo ID. The passenger's checked baggage is scanned by X-ray scanner 113, and the X-ray imagery thus produced is captured by Networked Surveillance Encoder 112, and subsequently appended to the Passenger's record in the Facial Database. An additional Networked Surveillance camera 111B images the passenger's baggage as it leaves the X-ray scanner, and the resulting image is appended to the networked Image Database. A networked explosives sensor 115 likewise produces data descriptive of the baggage, and is likewise appended to the networked Image Database.

[127] Figure 12 depicts the equipment at a typical security checkpoint used for passenger screening. Passengers arrive at the security checkpoint and deposit their carry-on baggage on the conveyor belt of X-ray scanner 123. At that time, they are photographed by networked surveillance camera 121A. The image is stored in the network's Image Database, and a networked Facial Processor derives a Facial Signature for the passenger. This data is appended to the existing record in the Facial Database representing that passenger. Additionally, at this time the passenger's photo ID and ticket are scanned into networked scanner 120A, and this data is appended to the passenger's file as well.

[128] A further networked surveillance camera may be used, if needed, at an inspection table, near the passenger metal detector, to capture an image of any personal items from the person's pockets or purse, or other personal luggage, during such an inspection. This image, as well, is appended to the passenger's record in the database. In addition to images from this scan of personal items, data from a networked explosives scanner, and scanned images of the passenger's luggage tag, may be added to the passenger's record in the database.

[129] Security personnel occasionally encounter personal items of an unknown nature, which may require evaluation and approval by qualified supervisors. To improve the speed of the process, supervisors may review real-time networked video of the personal items on the inspection table, and make necessary decisions without having to travel to the security checkpoint.

[130] As the passenger deposits his carry-on baggage onto the conveyor belt of X-ray scanner 123, networked surveillance camera 121B captures an image of the passenger's carry-on baggage, and appends it to the passenger's record in the Facial Database. As the passenger's carry-on baggage is scanned by X-ray scanner 123, networked surveillance encoder 124 captures the scanned image from x-ray scanner 123, and again appends it to the passenger's file. Networked surveillance camera 121C captures an image of the carry-on baggage as it leaves the X-ray scanner 123, and may optionally be positioned to capture an image of both the carry-on baggage as well as the passenger as they retrieve their carry-on baggage from the conveyor. Again, these captured images are appended to the passenger's file.

[131] Figure 13 depicts the apparatus used at a typical boarding gate. At scanner 130, the passenger's ticket and photo ID are scanned, and added to the passenger's database entry. Additionally, the passenger is photographed by networked surveillance camera 133. A facial signature from the passenger's photo ID, and a Facial Signature derived from camera 133's captured image, may be compared to verify the passenger's identity. Either or both of these Facial Signatures may additionally be compared with similar entries previously added to the passenger's database record, again verifying the passenger's identity.

[132] Figure 14 depicts an aircraft 140 being loaded with checked baggage. As baggage 143 is loaded onto the aircraft via conveyer 142, a networked surveillance camera 141 captures an image of the bag. In addition, a handheld barcode scanner 144 captures the data from the barcoded baggage tag. The bag's image is transferred, via the facility's security LAN, to the Image Database for storage. In addition, the baggage barcode is stored in the passenger's file. This allows subsequent matching of baggage, as loaded onto the aircraft, with baggage that had been previously matched to a known passenger.

[133] Figure 15 depicts apparatus installed on board a mass-transit vehicle, herein depicted as an aircraft 150. Several cameras, shown as 151, 152, and 153, are positioned to capture imagery of the aircraft interior. In particular, areas of interest are the entryway door(s), cockpit, and passenger area 154. Video or still-frame images thus captured are conveyed to a satellite communications radio 155, then to satellite 157 via aircraft antenna 156. From the satellite, images are forwarded to a satellite groundstation, as depicted in Figure 7.

[134] Images captured by on-board cameras 151 through 153 are forwarded to a networked Facial Processor, which extracts Facial Signatures from faces detected in the various images. These Facial Signatures may then be compared with those Facial Signatures of passengers known to be on the flight. In the case of a discrepancy, such as an 'unknown' face present on the flight, or conversely a 'known' face missing from the flight, appropriate security measures may be taken.

[135] While certain embodiments and features of the invention have shown and described in detail herein, it will be understood that the invention encompasses all modifications and enhancements within the scope and spirit of the following claims.